PRF73: PAYMENT DATA & PAYMENT CARD INDUSTRY (PCI) COMPLIANCE SERVICES

UPDATED: May 28, 2020

Contract #:	PRF73
MMARS MA #:	PRF73DesignatedCTR00
Initial Contract Term:	March 16, 2020 – January 10, 2025
Maximum End Date:	One 5-year extension to January 10, 2030
Current Contract Term:	March 16, 2020 – January 10, 2025
Contract Manager:	Kristine Hill-Jones - 617-973-2362- Kristine.Hill-Jones3@mass.gov
This Contract Contains:	Prompt Pay Discounts
UNSPSC Codes:	93-15-00 Public administration and finance services
Notes:	Contract documents are available on COMMBUYS. Search for PRF73.

***The asterisk is required when referencing the contract in the Massachusetts Management Accounting Reporting System (MMARS).**

Table of Contents:

(NOTE: To access hyperlinks below, scroll over desired section and CTL + Click)

Contract User Guide for PRF73

TIP: To return to the first page throughout this document, use the CTL + Home command.

Contract Summary

This Statewide Contract, **PRF73 Payment Data & Payment Card Industry (PCI) Compliance Services** provides a full suite of compliance audits, quality assurance reviews, and testing for Payment Card Industry (PCI) compliance, to protect personally identifiable information and other sensitive data. This Statewide Contract has pre-qualified vendors for two categories which are meant to replace Categories **A** (QSA) and **B** (ASV) of PRF56DesignatedOSC01 - Information Management, Data Security, and Payment Card Industry Compliance.

As this Statewide Contract is procured under the authority of the Office of the Comptroller (CTR) to implement State Finance Law and prescribe fiscal accountability, State Department merchants must use this Statewide Contract to procure the services of QSA professionals and ASVs for Payment Card Industry Council Data Security Standards and for security compliance audits (in any branch of government) as prescribed in the Non-Tax Revenue - Revenue Collection Data Security Policy. These services may not be independently procured under separate general procurement authority. Any Commonwealth Department that accepts credit or debit cards is required to comply with the merchant requirements published by the Payment Card Industry Security Standards Council in addition to any other state or federal laws, regulations or policies related to the storing, processing or transmitting of cardholder data which is considered PII. Depending on the Department's merchant level and volume of transactions, a Department may be required to complete a PCI DSS Self-Assessment Questionnaire (SAQ) or a Report on Compliance (ROC) and file with their merchant bank or card processor, conduct quarterly vulnerability scans, penetration tests, and facilitate periodic validation of Payment Card Industry Data Security Standards compliance.

Data Security compliance helps merchant Eligible Entities improve the safekeeping of cardholder information by tightening overall security standards and information management to:

- Minimize vulnerabilities;
- Reduce the chance of breaches, fraud, and financial loss;
- Ensure the security of the Commonwealth of Massachusetts' e-commerce applications; and
- Seek opportunities to limit scope and reduce system and protocol vulnerabilities.

In addition, the Commonwealth of Massachusetts, pursuant to G.L. c. 93H and 93I has responsibility to safeguard data deemed Personally Identifiable Information (PII), in addition to protections mandated by other state and federal statutes and regulations for other types of confidential data.

The duties to protect PII under G.L. c. 93H and 93I and other authority apply equally to both PCI covered data (credit card holder data) and non-PCI covered data (bank accounts, ACH and all other personally identifiable information (PII)). At this time, the Payment Card Industry Council mandates a formal PCI Compliance process to validate DSS for all merchants. For Executive Departments, an Enterprise self-assessment process has been completed to document the types of confidential and PII data collected and retained by Departments, and the Executive Office of Technology services and Security (EOTSS) has published Enterprise Security Standards for the protection of confidential, sensitive and PII.

By policy, the Office of the Comptroller and the Executive Office of Technology services and Security (EOTSS) have mandated that all Commonwealth Department merchants provide annual certification of Data Security compliance even if an independent audit is not required by the Payment Card Security Standards Council or the Eligible Entity's merchant bank, acquirer, or card processor. See Non-Tax Revenue – Revenue Collection Data Security Policy (CTR website). This additional requirement is necessary to ensure that Department merchants are taking the necessary steps to annually verify continued Data Security compliance and have an independent evaluation that vulnerabilities have been identified and mitigated to prevent a data breach under G.L. c. 93H and c. 93I or the Payment Card Industry Security Standards Council standards.

Annual budgets for any Eligible Entity accepting revenue should ensure sufficient funding to maintain continued data security compliance, and reduction in budgeted funds will not support any failure to maintain continued compliance.

Contract Categories

This contract includes 2 categories of services as listed below.

Category 1 vendors have been approved by the Payment Card Industry Security Standards Council to provide Qualified Security Assessor (QSA) and related QSA consulting services. Only approved QSAs can perform PCI Compliance validation. These vendors offer a full suite of assessment and consulting services for Eligible Entities receiving revenue through credit cards to ensure PCI compliance and validation.

Category 2 vendors have been approved by the Payment Card Industry Council to provide Approved Scanning Vendor (ASV) services. An ASV is an organization with a set of security services and tools to conduct external vulnerability scanning services to validate adherence with the requirements of the PCI DSS.

Category 1: PCI Council Approved Quality Security Assessors (QSAs) and related QSA Consulting Services.
Category 2: PCI Council Approved Scanning Vendors (ASVs) including Vulnerability Testing and Other Security Compliance Scans and Testing.

Benefits and Cost Savings

Statewide contracts are an easy way to obtain benefits for your organization by leveraging the Commonwealth's buying power, solicitation process, contracting expertise, vendor management and oversight, and the availability of environmentally preferable products.

Find Bid/Contract Documents

To find all contract-specific documents, including the Contract User Guide, RFR, specifications, price sheets and other attachments, visit COMMBUYS.com and search for PRF73 in the "Contract/Blanket description" field to find related Master Blanket Purchase Order (MBPO) information.

For PRF73 - Payment Data & Payment Card Industry (PCI) Compliance Services Master Contract Record - PO-20-1080-OSD03-SRC02-19401

For Executive Departments -PRF73 - Payment Data & Payment Card Industry (PCI) Compliance Services Solicitation Enabled - PO-20-1080-OSD03-SRC02-19403

For vendor MBPO related information see the "Vendor List and Information" table in the in this guide.

Who Can Use This Contract

Applicable Procurement Law

Executive Branch Goods and Services: MGL c. 7, § 22; c. 30, § 51, § 52; 801 CMR 21.00.

Eligible Entities

This Statewide Contract is open to the following Eligible Entities as found on the Who Can Use Statewide Contracts webpage.

Each eligible entity is responsible for executing its own SOW and paying its own invoices for goods and/or services acquired from this Contract.

Subcontractors

Prior approval of the department is required for any subcontracted service of the Contract. Contractors are responsible for the satisfactory performance and adequate oversight of their subcontractors.

Pricing, Quote and Purchase Options

Purchase Options

The purchase options identified below are the only acceptable options that may be used on this contract:

This is a fee for service contract.

Pricing Options

Fixed Pricing: Contract pricing has been negotiated. Max hourly rates are attached within the **PRF73** posting in COMMBUYS. Vendors may offer prices less than the listed price but may not exceed the listed price.

Product/Service Pricing and Finding Vendor Price Files

Pricing may be found by clicking on individual vendor MBPOs on the Vendor Information page.

When contacting a vendor for this statewide contract, always reference **PRF73** to receive contract pricing.

Setting Up a COMMBUYS Account

COMMBUYS is the Commonwealth's electronic Market Center supporting online commerce between government purchasers and businesses. If you do not already have an account, contact the COMMBUYS Help Desk to set up a COMMBUYS buyer account for your organization: (888)-627-8283 or COMMBUYS@mass.gov.

*Per **801 CMR 21.00**, Executive Branch Departments must use established statewide contracts for the purchase of commodities and services. Specifically, Executive Departments are required to use OSD's statewide contracts, including designated statewide contracts, if available, for their specific commodity and service needs. Exceptions will only be permitted with prior written approval from the OSD designee the Office of the Comptroller.*

Quick Search in COMMBUYS

Log into COMMBUYS, and use the Search box on the COMMBUYS header bar to locate items described on the MBPO or within the vendor catalog line items. Select Contract/Blanket or Catalog from the drop-down menu.

How To Purchase From The Contract

Solicit quotes and select and purchase quoted item in COMMBUYS

COMMBUYS has solicitation of bids enabled. This COMMBUYS functionality provides a mechanism to easily obtain quotes, as specified by the Contract. The buyer would create a Release Requisition, and then convert it to a Bid. After approval by the buyer approving officer, the bid is then sent to selected vendors to request quotes. Buyers must include "PRF73 RFQ" when entering information in the Description field. Buyers must also include the **PRF73** Statement of Work (SOW)/Quote Form when engaging vendors on **PRF73 (see instructions below)**.

For a description of how to complete this purchase in COMMBUYS, visit the *Job Aids for Buyers* webpage, and select: The *COMMBUYS Purchase Orders* section, and choose the *How to Create a Solicitation Enabled Bid Using a Release Requisition* job aid or one of the quick reference guides.

Obtaining Quotes

Executive Departments must use COMMBUYS to solicit quotes and engage in services. Other Eligible Entities may contact any of the Vendors on this Statewide Contract directly to inquire about engaging their services.

Contract users should always reference **PRF73** when contacting vendors to ensure they are receiving contract pricing. Quotes should be awarded based on best value.

When engaging Vendors on the Contract, Eligible Entities must use the PRF73 Payment Data & Payment Card Industry (PCI) Compliance Services Statement of Work (SOW)/Quote Form. When selecting a contractor, Eligible Entities should review the Contractor Response Document and Pricing Document. The SOW/Quote Form, Contractor Response Document and Pricing Document can be found as an attachment on the PRF73 COMMBUYS posting and on the CTR Website.

Instructions for Requesting Quotes and Completing SOW

1. **PRF73 Payment Data & Payment Card Industry (PCI) Compliance Services Statement of Work (SOW)/Quote Form.** For purposes of this Statewide Contract, Eligible Entities are required to pre-populate the **PRF73 Payment Data & Payment Card Industry (PCI) Compliance Services (SOW)/Quote Form** posted on COMMBUYS for this contract with the proposed work to be performed under an engagement. For Statewide Contract management purposes, CTR may request periodic reports of all engagements at any time from Eligible Entities and Vendors.

2. Competitive Quotes. The PRF73 Data Security Statement of Work (SOW)/Quote Form should be sent by the Eligible Entity to multiple Contractors authorized for the category of performance sought, unless the Eligible Entity is currently engaged for the same work under prior engagement with one of the awarded Vendors. Eligible Entities are encouraged to submit quotes to all Contractors in a category to obtain the broadest range of performance and competition. Note that Contractors are authorized to provide performance solely in their authorized performance categories.

3. The PRF73 Payment Data & Payment Card Industry (PCI) Compliance Services (SOW)/Quote Form is then returned completed (unexecuted) from the Contractors interested in bidding on the engagement to the Eligible Entity.

4. The Eligible Entity reviews the Contractor's Response Document including pricing (RFR Response **Template Posted on COMMBUYS)** along with the **PRF73 Payment Data & Payment Card Industry (PCI) Compliance Services SOW/Quote FORM** to select the best value Contractor for the engagement. Selection may include interviews and negotiations to finalize the engagement performance terms and pricing. Pricing for any SOW engagement may not be greater than prices posted under the Contract and Contractors are limited to providing only the services within the authorized category(ies) for that Contractor.

5. **Updated/Finalized SOW**. Once a Contractor has been selected, the details of the engagement (services to be performed, timeline or schedule of performance completion dates and pricing) should be finalized by updating the SOW that is executed by authorized signatories of the Vendor and Eligible Entity. Eligible Entities may request a copy of the Contractor Authorized Signatory Listing (CASL) from CTR at PRF73PCICompliance@mass.gov that is used to validate authorized signatories for a Contractor. The SOW is not a separate contract but an engagement under the Statewide Contract **PRF73DesignatedCTR00** incorporated by reference herein, and serves as the scope of performance and budget for this engagement. Additional conflicting contract terms and conditions may not be included, referenced or attached to the SOW.

6. **Materials Incidental to the Service.** As this is an audit service, Eligible Entities will negotiate the scope of the engagement and provide access to the systems, protocols, staff and information necessary to perform the audit. Eligible Entities, depending upon the engagement, may be asked to identify team and primary contacts, payment data flow, network diagram, outward facing IP addresses and wireless networks, identify if the Eligible Entity is using its own payment application or a third-party application, policies and internal controls for maintaining information security and data security compliance.

7. **Purchase Options**: Bidders will be paid based upon reaching established scheduled milestones, submission of required reports, data or other documentation in accordance with required scope of service and fees. Eligible Entities reserve the right to withhold payment for any scheduled milestone that is not met until properly completed. Eligible Entities also reserve the right to apply a retainage on all payments to ensure delivery of services under the terms of the contract.

Instructions for MMARS Users

PRF73DesignatedCTR00 MMARS users must reference the MA number in the proper field in MMARS when placing orders with any contractor.

Payments by State Departments

All payments made by State Departments under the state accounting system MMARS MUST be made using the Master Agreement (MA) for this Statewide Contract**: MA-OSD- PRF73DesignatedCTR00**.

Other Discounts

Prompt Pay Discounts: A discount given to the buyer if paid within a certain time period. These discounts may be found in the Vendor List and Information section below. Prompt Pay Discount is also located on COMMBUYS as attachment to **PRF73**. All discounts offered will be taken in cases where the payment issue date is within the specified number of days listed by vendor and in accordance with the Commonwealth's Bill Paying Policy. Payment days will be measured from the date goods are received and accepted / performance was completed OR the date an invoice is received by the Commonwealth, whichever is later to the date the payment is issued as an EFT (preferred method) or mailed by the State Treasurer. The date of payment "issue" is the date a payment is considered "paid" not the date a payment is "received" by a Contractor.

For non-MMARS entities, the Prompt Pay Discount may be deducted from the amount the Vendor invoiced, based on when your agency received the invoice and when the vendor will receive the payment. Please be conservative in estimated how long it will take for a check issued by your agency to be received by the vendor, to avoid having to remit the amount of any Prompt Pay Discount that was not warranted.

Additional Information

General Background

Payment Card Industry Council Security Standards for Acceptance of Credit and Debit Cards
All Commonwealth Entities that currently accept credit or debit card payments are considered "merchants" or "submerchants" and are required to validate data security compliance. Compliance standards are set by the Payment Card Industry Security Standards Council and compliance is enforced by the payment card brands for each merchant level, which depends upon the volume of transactions.

> *The Payment Card Industry Data Security Standard (PCI DSS) secures cardholder data that is stored, processed or transmitted by merchants and other organizations. The standard is managed by the PCI Security Standards Council (PCI SSC) and its founders, the global payment brands: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.*
>
> *The PCI Data Security Standard and supporting documents represent a common set of industry tools and measurements to help ensure the safe handling of sensitive information. The standard provides an actionable framework for developing a robust account data security process - including preventing, detecting and reacting to security incidents. To reduce the risk of compromise and mitigate its impacts if it does occur, it is important that all*

entities storing, processing, or transmitting cardholder data be compliant.
(https://www.pcisecuritystandards.org/security_standards/index.php)

Contract File Additional Documents

Copies of the Commonwealth Terms and Conditions, Standard Contract Form, Contractor Authorized Signatory Listing (CASL), Prompt Payment Discount Terms (in SCF) are available from CTR and can be emailed to an Eligible Entity upon request to complete the Contract File (for audit purposes) and to validate signatories when executing SOWs. Please email PRF73PCICompliance@mass.gov for these documents, and with any questions related to using the SOW and Statewide Contract.

Additional Reporting Requirements for Contract Management

For Statewide Contract management purposes CTR may request periodic reports of all engagements under the Statewide Contract at any time from Eligible Entities and Vendors.

Performance and Payment Time Frames Which Exceed Contract Duration

All agreements for services entered into during the duration of this Contract and whose performance and payment time frames extend beyond the duration of this Contract shall remain in effect for performance and payment purposes (limited to the time frame and services established per each written agreement). No written agreement shall extend more than 24 months beyond the current contract term of this Statewide Contract as stated on the first page of this contract user guide. No new agreements for services may be executed after the Contract has expired.

Strategic Sourcing Team Members

- Thomas Smith-Vaughan, CTR
- John Scully, CTR
- Peter Scavotto, CTR
- Kristine Hill-Jones, CTR
- Patricia Davis, CTR
- Parris Kyriakakis, CTR
- Gary Foster, MBTA
- John Merto, EOTSS
- Andrew Russell, UMS
- Kathryn White, UMS
- William Morrison, MAS

Contract User Guide for PRF73

Vendor List and Information*

Vendor	Master Blanket Purchase Order #	Contact Person	Phone #	Email	Categories	Discounts (PPD, Dock Delivery, Other)	MBE MWBE WBE Veteran
Master Contract Record PO	PO-20-1080-OSD03-SRC02-19401	Kristine Hill-Jones	1-617-973-2362	Kristine.Hill-Jones3@mass.gov	N/A	N/A	N/A
Solicitation Enabled PO	PO-20-1080-OSD03-SRC02-19403	Kristine Hill-Jones	1-617-973-2362	Kristine.Hill-Jones3@mass.gov	N/A	N/A	N/A
Compass IT Compliance, LLC	PO-20-1080-OSD03-SRC02-19394	William DePalma	1-401-353-3024	wdepalma@compassitc.com	1, 2	10 days 2.5%, 15 days 2.0%, 20 days 1.0%	N/A
RSI Systems, Inc. DBA RSI Security	PO-20-1080-OSD03-SRC02-19395	Lucy Phan	1-858-999-3030	bids@rsisecurity.com	1, 2	N/A	N/A

*Note that COMMBUYS is the official system of record for vendor contact information.